Date of Approval: **April 08, 2021**

PIA ID Number: **5849**

SYSTEM DESCRIPTION

Enter the full name and acronym for the system, project, application and/or database.

Withholding Compliance System (WHCS), WHCS

Is this a new system?

No

Is there a PCLIA for this system?

Yes

What is the full name, acronym and milestone of the most recent PCLIA?

Withholding Compliance System [3182]

What is the approval date of the most recent PCLIA?

3/29/2018

Changes that occurred to require this update:

Expiring PCLIA

Were there other system changes not listed above?

No

What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym.

Small Business Self Employed (SBSE) Technology Governance Board

Current ELC (Enterprise Life Cycle) Milestones:

Operations & Maintenance (i.e. system is currently operational)

Is this a Federal Information Security Management Act (FISMA) reportable system?

Yes

GENERAL BUSINESS PURPOSE

What is the general business purpose of this system? Provide a clear, concise description of the system, application or database, the reason for the system, and the benefits to the IRS to use the information, and how the information will be used.

The mission of the Withholding Compliance Program (WHC) is to ensure that taxpayers who have serious under-withholding problems are brought into compliance with federal income tax withholding requirements. WHC uses Form W-2 Wage and Tax Statement (W-2) information to identify taxpayers with insufficient withholding that result in tax compliance problems. The goal is to correct withholding to ensure that taxpayers have enough income tax withheld to meet their withholding tax obligations. In instances where a serious under-withholding problem exists for a particular taxpayer, IRS may issue a notice, commonly known as a "lock-in letter" to the employer. This notice directs the employer to disregard the taxpayer's Form W-4 and withhold using the marital status and number of allowances specified by the Service. WHC cases are housed in the Withholding Compliance System (WHCS), a database application owned by the Small Business/Self-Employed (SB/SE) Business Unit. The application resides on the IBM mainframe at the Enterprise Computing Center - Martinsburg (ECC-MTB) and does not directly interface with any other systems external to the IRS. All input to the WHCS application is obtained via batch processes that pull information from the Individual Master File (IMF) and Payer Master File (PMF). The Withholding Compliance System Case Creation (WHCSCC) utilizes the Form W-2 to identify employees with a potential under-withholding problem that could be causing tax compliance problems. The system enables the Service to determine when employers are complying with the instructions that the IRS provides to them. WHCSCC creates compliance cases by matching W2s to the Individual Master File. It is a component of the Withholding Compliance System (WHCS). WHCS provides a means to monitor and control information related to the WHC case inventory. Records contain case-related personally identifiable information (PII). WHCS users can add, update, query, close, and maintain case information such as case actions, decisions made, and letters issued to taxpayers and/or employers.

PII DETAILS

Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any other type of Sensitive but Unclassified (SBU) information or PII such as information about IRS employees or outside stakeholders?

Yes

Does the system use, collect, receive, display, store, maintain, or disseminate Social Security Numbers (SSN's) or tax identification numbers (i.e. last 4 digits, etc.)?

Yes

What types of tax identification numbers (TIN) apply to this system?

Social Security Number (SSN)

List the approved Treasury uses of the SSN:

Legal/statutory basis (e.g. where collection is expressly required by statute)

Delivery of governmental benefits, privileges, and services

Explain why the authorized use(s) above support the new or continued use of SSNs (or tax identification numbers).

The WHCS system requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns.

Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN's (or tax identification numbers).

The Office of Management and Budget Circular A-130 requires that federal agencies develop a mitigation or elimination strategy for systems that use SSNs, which the Service continues to develop strategies to meet. An exception to that requirement is when the SSN is uniquely needed to identify a user's record. WHCS requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer at this time.

Employer Identification Number

Other Taxpayer Identification Number

Does this system use, collect, receive, display, store, maintain or disseminate other (non-SSN) PII (i.e. names, addresses, etc.)?

Yes

Specify the PII Elements:

Name
Mailing address
Phone Numbers
Tax Account Information

Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?

Yes

Specify the types of SBU from the SBU Types List:

Agency Sensitive Information Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission.

Official Use Only (OUO) or Limited Official Use (LOU) Information designated as OUO or LOU is information that: is exempt under one of the statutory Freedom of Information Act exemptions; is prohibited by other laws or regulations; would significantly impede the agency in carrying out a responsibility or function; or would constitute an unwarranted invasion of privacy.

Protected Information Information which if modified, destroyed or disclosed in an unauthorized manner could cause: loss of life, loss of property or funds by unlawful means, violation of personal privacy or civil rights, gaining of an unfair procurement advantage by contractors bidding on government contracts, or disclosure of proprietary information entrusted to the Government.

Are there other types of SBU/PII used in the system?

No

Cite the authority for collecting SBU/PII (including SSN if relevant).

PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, & 6012e(a)

SSN for tax returns and return information is Internal Revenue Code Section 6109

Has the authority been verified with the system owner?

Yes

BUSINESS NEEDS AND ACCURACY

Explain the detailed business needs and uses for the SBU/ PII, and how the SBU / PII is limited only to that which is relevant and necessary to meet the mission requirements of the system. If SSNs (or tax identification numbers) are used, explicitly explain why use of SSNs meets this criteria. Be specific.

SSN - is used to identify the individual taxpayers. Address, City, State and Zip of taxpayer - is used to send out WHC letters. Employer Identification Number (EIN) - is used to identify taxpayer's employer Address, City, State and Zip Code of Employer - is used to send out WHC letters Tax Account Data - is used to identify taxpayer as Balance Due (BD) of Nonfiler (NF)

How is the SBU/PII verified for accuracy, timeliness and completion?

Data is verified through Masterfile prior to importing into the WHCS databases. Additionally, any changes or modifications are based on direct contact with the taxpayer.

PRIVACY ACT AND SYSTEM OF RECORDS

The Privacy Act requires Federal agencies that maintain a system of records to publish systems of records notices (SORNs) in the Federal Register for records from which information is retrieved by any personal identifier for an individual who is a US citizen or an alien lawfully admitted for permanent residence. The Privacy Act also provides for criminal penalties for intentional noncompliance.

Does your application or this PCLIA system pertain to a group of any record from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence? An identifier may be a symbol, voiceprint, SEID, or other personal identifier that is used to retrieve information.

Yes

Identify the Privacy Act SORN(s) that cover these records.

IRS 24.030 Customer Account Data Engine Individual Master File

IRS 24.046 Customer Account Data Engine Business Master File

IRS 42.021 Compliance Programs and Projects Files

IRS 34.037 Audit Trail and Security Records

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

Official Use Only

INCOMING PII INTERFACES

Does the system receive SBU/PII from other systems or agencies?

Yes

Does the system receive SBU/PII from IRS files and databases?

Yes

Enter the files and databases:

System Name: Payer Masterfile
Current PCLIA: Yes
Approval Date: 5/4/2020
SA&A: Yes
ATO/IATO Date: 12/4/2015

System Name: Individual Masterfile
Current PCLIA: Yes
Approval Date: 3/4/2020
SA&A: Yes
ATO/IATO Date: 11/26/2019

Does the system receive SBU/PII from other federal agency or agencies?

Yes

For each federal interface, identify the organization that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Name: Social Security Administration
Transmission Method: File Transfer
ISA/MOU: Yes

Does the system receive SBU/PII from State or local agency (-ies)?

No

Does the system receive SBU/PII from other sources?

No

Does the system receive SBU/PII from Taxpayer forms?

No

Does the system receive SBU/PII from Employee forms (e.g. the I-9)?

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

Yes

Does this system disseminate SBU/PII to other IRS Systems?

Yes

Identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name: Correspondex (IDRS)
Current PCLIA: Yes
Approval Date: 10/1/2018
SA&A: Yes
ATO/IATO Date: 1/17/2018

Identify the authority.

Letters 2800, 2801, 2802 are generated under Regulations in 26 CFR Part 31, Employment Taxes and Collection of Income Tax at Source and provide guidance for implementation of IRC Section 3402.

For what purpose?

The Letter 2800 directs employers to adjust a taxpayer's withholding to the rate specified by IRS and also establishes the delivery and notification requirements for the employer for IRC Section 3403 penalties, should the employer fail to properly withhold after the Letter 2800 has been delivered.

Does this system disseminate SBU/PII to other Federal agencies?

No

Does this system disseminate SBU/PII to State and local agencies?

No

Does this system disseminate SBU/PII to IRS or Treasury contractors?

No

Does this system disseminate SBU/PII to other Sources?

No

PRIVACY SENSITIVE TECHNOLOGY

Does this system use social media channels?

No

Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?

No

Does the system use cloud computing?

No

Does this system/application interact with the public?

No

INDIVIDUAL NOTICE AND CONSENT

Was/is notice provided to the individual prior to collection of information?

Yes

How is notice provided? Was the individual notified about the authority to collect the information, whether disclosure is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects on the individual, if any, if they decide not to provide all or any of the requested information?

Information comes from Masterfiles and Payor Masterfile as well as the Form W-2 file received from the Social Security Administration (SSA). Taxpayers are not provided notice until we actually select them for a WHC Lockin Letter. A privacy notice is provided on both

the W-2 and W-4 forms. Notice, consent and due process are provided in the tax forms instructions filed by the taxpayer, and pursuant to 5 USC.

Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information?

No

Why not?

Regulations in 26 CRF Part 31, Employment Taxes and Collection of Income Tax at Source provide guidance for implementation of IRC Section 3402.

How does the system or business process ensure 'due process' regarding information access, correction and redress?

Any corrections to the data are based on contact from/with the Taxpayer.

INFORMATION PROTECTION

Identify the owner and operator of the system (could be IRS owned and Operated; IRS owned, contractor operated; contractor owned and operated).

IRS Owned and Operated

The following people have access to the system with the specified rights:

IRS Employees

Users: Read Write

Managers: Read Write

How is access to SBU/PII determined and by whom?

Data access to the WHC application is restricted based on the principle of least privilege and separation of duties. Access is granted on a need-to-know basis. WHCS personnel are required to apply for access using the Online 5081 (OL5081) enrollment process which requires that an authorized manager approve access requests on a case by case basis. Upon approval, WHCS users are assigned role based user accounts comprising unique role privileges and responsibilities. Management determines which employees are selected to work these cases.

RECORDS RETENTION SCHEDULE

Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) approved a Records Control Schedule (RCS, IRS Document 12990) for the retention and destruction of official agency records stored in this system?

Yes

How long are the records required to be held under the corresponding GRS or RCS, and how are they disposed of? In your response, please provide the GRS or RCS chapter number, the specific item number, and records series title.

Any records generated and maintained by WHCS will be managed according to requirements defined in IRM 1.15.1 and 1.15. and will be destroyed using IRS Records Control Schedule (RCS) 29, Item 85 (5) Job N158-07-9 AUTHORIZED DISPOSITION Delete 3 years after lock-in is released or 10 years after lock-in date, per precedence. All records residing in the WHCS system will be purged in accordance with approved retention policies aligned with National Archives approval.

SA&A OR ASCA

Has the system been through SA&A (Security Assessment and Authorization) or ASCA (Annual Security Control Assessment)?

Yes

What date was it completed?

10/26/2020

Describe the system's audit trail.

The following are the details aligned with WHCS audit events as interrupted and annotated in the ACR resultant IRM 10.8.1 Auditable Event: Use of identification and authentication mechanisms (e.g., user id and password) (Success, Failed), Remote access outside of the corporate network communication channels (e.g. Modems, dedicated Virtual Private Network (VPN)) and all dial-in access to the system (Success, Failed), Application critical record changes (Success, Failed), Creating Files (Success, Failed), Deleting Files (Success, Failed), Change of file or user permissions or privileges (use of Globally Unique Identifier (GUID), Universally Unique Identifiers (UUID), Linux chown command, Set User ID (SUID), etc.) (Success, Failed), Command line changes and queries made to the system or application (Success, Failed), Changes made to an application or database by a batch file (Success, Failed), Changes to database or application records, where the application has been bypassed to produce the change (via a file or other database utility, batch process, or manual intervention) (Success, Failed), All system and data interactions concerning Personally

Identifiable Information (PII) and Sensitive But Unclassified (SBU), to include Taxpayer data (Success, Failed), Employee and Contractor transactions that add, delete, modify or research: a tax filer's record, an employee's record (personnel or financial), and Access to Employee User Portal (EUP), Opening and/or closing of Files (Success, Failed), Program Execution (Success, Failed). Logs onto the system (Success, Failed), Log off of system (Success), Change of Password (Success, Failed), Switching account or running privileged actions from another account (e.g., Linux/Unix SU or Windows RUNAS) (Success, Failed), Creation or modification of superuser groups (Success, Failed), All system administrator (SA) commands, while logged on as an SA, All privileged user actions, Clearing of the audit log file (Success, Failed), Startup and shut down of audit functions (Success, Failed),

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

Yes

Where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)?

An ISCM ATO Memo, System tests and plans are stored in the Treasury Financial Information Management System (TFIMS), CSAM and DocIT, an IRS repository.

Were all the Privacy Requirements successfully tested?

Yes

Are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved?

No

Describe what testing and validation activities have been conducted or are in progress to verify and validate that the applicable Privacy Requirements (listed in header) have been met?

All the customer configurable security controls are implemented as intended and documented in the WHCS System Security Plan (SSP).

SBU DATA USE

Does this system use, or plan to use SBU Data in Testing?

No

NUMBER AND CATEGORY OF PII RECORDS

Identify the number of individual records in the system for each category:

IRS Employees: Not Applicable

Contractors: Not Applicable

Members of the Public: More than 1,000,000

Other: No

CIVIL LIBERTIES

Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?

No

Is the system information used to conduct 'data-mining' as defined in the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?

No

Will this system have the capability to identify, locate, and monitor individuals or groups of people?

No

Does computer matching occur?

Yes

Does your matching meet the Privacy Act definition of a matching program?

Yes

Can the business owner certify that it meets requirements of IRM 11.3.39, Disclosure of Official Information, Computer Matching & Privacy Protection Act?

Yes

ACCOUNTING OF DISCLOSURES

Does the system include or require disclosure of tax or employee information to anyone other than IRS employees in the performance of their duties, or to the person to whom the information pertains or to a 3rd party pursuant to a Power of Attorney, tax or Privacy Act consent?

No